UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/072,597	02/05/2002	Paul A. Cronce	2401P	1789

57580 7590 01/14/2008

STRATEGIC PATENT GROUP, P.C.
P.O. BOX 1329
MOUNTAIN VIEW, CA 94042

EXAMINER	
BAYAT, BRADLEY B	
ART UNIT	**PAPER NUMBER**
3621	

MAIL DATE	DELIVERY MODE
01/14/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/072,597
Filing Date: February 05, 2002
Appellant(s): CRONCE, PAUL A.

Stephen Sullivan
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 9/17/2007 appealing from the Office action mailed 1/23/2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The following are the related appeals, interferences, and judicial proceedings known to the examiner which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal:

Co-pending application number 10/080,639 before the BPAI.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Venkatesan et al. (hereinafter Venkatesan), US Patent 6,898,706 B1.

As per the following claims, Venkatesan discloses:

1. A method for the delivery of secure software license information to authorize use of a software product, the method comprising the steps of:

(a) associating with a software publisher a private and public key pair, wherein the software publisher provides the software product and includes a software program and an authorization program within the software product (fig 5, publisher 330 downloads file encrypted, including watermark keys and fingerprinted for client PC 520)

(b) associating a product private key and public key with the software product, wherein at least one of the product private and public keys is digitally signed by the publisher private key and including the product private and public keys with the authorization program (fig 5, upon payment by user, publisher issues and downloads to user electronic license with usage rights including secret key 550);

(c) upon invocation of the software product on a computer, (i) generating by the authorization program a license request containing user and product information, (ii) digitally signing the license request with the product private key, and (iii) transferring the signed license request to a key authority (figure 3, certificate authority 307A signs with private key becoming part of the secure container for transfer to the key authority in figure 4);

(d) in response to the key authority receiving the signed license request, (i) generating a license using data extracted from the license request and license terms, (ii) signing the license with the publisher private key, and (iii) transmitting the signed license to the authorizing program (figure 13A, license verification, object decryption and enforcement 1300); and

(e) validating the signed license using the publisher public key, and using the license terms to control the use of the software product (figure 13A, enforcer process 1320, fig 13B instruct access in accordance with usage conditions 1380).

2. The method of claim 1 further including the step of providing the publisher public key as a certificate (fig 12, publisher's public key certificate1220).

3. The method of claim 2 further including the step of providing the product public key as a certificate (fig 11, license generation and download 1122 including PID and certified public key).

4. The method of claim 1 further including the step of providing the license in a data exchange format (fig 5, client PC and Publisher data exchange 545 and 555).

5. The method of claim 4 further including the step of using XML as the data exchange format (column 11, lines 1-23, note that XML encoding may occur within HTML content; XML DTD describes a subset of HTML 4.0 for embedded use within other XML).

6. The method of claim 1 further including the step of using the license returned from the key authority to deliver additional key information to the computer (fig 13A, enforcer process 1320).

7. The method of claim 1 wherein step (d) further includes the step validating the license request using digital certificates (fig 11, computer ID of client PC 1122).

8. The method of claim 1 wherein step (e) further included the step of validating the license response using digital certificates (fig 11, computer ID of client PC 1122).

9. The method of claim 1 wherein step (e) further included the step of validating the license using the product information in the license, including product ID and publisher ID (figure 11, product Id and publisher 's symmetric encryption key 1122).

10. The method of claim 9 further including the step of transferring license terms to a separate security device for controlling the use of the software product (fig 5, encrypted store 610 includes license database 570 and object store 580).

11. The method of claim 1 wherein step (e) further included the step of preventing use of the software product on a different computer than that used to generate the license request by using a machine fingerprint embedded in the license request (fig 5, fingerprint for client PCj 520).

Claims 12-15 are directed to a method as recited above and are rejected as above.

16. A method for the delivery of secure software license information to authorize use of a software product, the method comprising the steps of:

a. associating with the software product to be authorized an authorization program and a set of certificates, including a publisher certificate and a product certificate, wherein each certificate contains a public key and is associated with a private key of a public/private key pair, wherein the product certificate is signed by the private key associated with the publisher certificate (figure 12 and associated text);

b. upon invocation of the software product on a computer, generating by the authorization program a formatted license request containing user and product information, signed using the private key associated with the product certificate (fig 11, client license request 1110);

c. transmitting the license request to a key authority in conjunction with a financial transaction (fig 11, request includes CID, client's public key, usage rights and payment information 1115);

d. generating by the key authority a formatted license that includes license terms, and user and product information extracted from the license request, wherein the license is signed with the publisher private key associated with the publisher certificate (fig 11, upon authorization of payment generating license 1122);

e. transmitting the signed license to the authorizing program (fig 11, transmit license to publisher's web server 1124); and

f. validating by the authorization program the license using the publisher and certificate authority certificates and the user and product information contained within the license document, whereby the validation using the publisher and certificate authority certificates establish a trusted link back to the certificate authority (fig 13 A license verification, object decryption and enforcement 1300, 1320) and;

g. using the license terms to control the use of the software product on the computer (fig 13B instruct use in accordance with rights and access 1380).

17. The method of claim 16 further including the step of formatting the license request and license documents using the proposed signed XML standard definition (column 11, lines 1-23, note that XML encoding may occur within HTML content; XML DTD describes a subset of HTML 4.0 for embedded use within other XML).

18. The method of claim 16 further including the step of signing the product certificate using the publisher's private key, and signing the publisher certificate using the certificate authority's private key, thus establishing a trusted link from the product certificate back to the certificate authority (fig 15, 16 and associated text)

19. The method of claim 16 further including the step of signing the license request using the product private key, and including within the license request the product certificate (fig 11, step 1115).

20. The method of claim 16 further including the step of including financial transaction information within the license request (fig 11, step 1115)

21. The method of claim 20 further including the step of including financial transaction information within the license response (fig 11, step 1122).

22. The method of claim 16 wherein step (g) further includes the step of transferring the license terms to a separate security device for controlling the use of the software product (fig 11, step 1124 publisher's web server downloads license to EC 610).

23. The method of claim 16 wherein step (g) further includes the step of preventing use of the software product on a different computer than that used to generate the license request by using a machine fingerprint embedded in the license request (fig 5, fingerprint 520).

Claims 24-26 are directed to a method as recited above and are rejected as above.

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially

teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

(10) Response to Argument

i) Claims 1-23 are clearly anticipated by Venkatesan

First, as per claims 1, 12 and 16 Appellant contends that "Venkatesan fails to teach or suggest that the software object, or part thereof, that has been downloaded to a client PC generates a license request (Brief at p. 15)." In response to Appellant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which Appellant relies upon are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In fact, the language of claim 1 recites, "upon invocation of the software product on a computer, i) generating by the authorization program a license request..." The language of the claim makes no reference to a software object that has been downloaded to a client PC generates a license request. Regardless, the cited reference discloses that the target object intended for download "may constitute an active software object, such as an executable program (column 11, lines 8-10)." In order to access the "locked" file, upon initiation of a download, a request to obtain a license certificate is facilitated to obtain the embedded watermark value and allow the DRM system to unlock the file (column 11, lines 14-41).

In response to Appellant's argument on page 16 of the brief that "because the generation of the license request is manually initiated by the user interacting with the PC through a Web browser," the reference fail to show certain features of Appellant's invention, it is noted that the

features upon which Appellant relies (i.e., automatic initiation of a license request without user interaction) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Regardless, the cited reference as discussed above provides an alternative embodiment "[w]ith respect to active objects, i.e., executable programs, the enforcer is preferably situated within an operating system itself executing in the client PC (column 14, lines 52-54)."

Appellant further contends that the "enforcer" in the cited reference "cannot be considered analogous to the authorization program (Brief at p. 16)." As illustrated in Figure 8 step 870, the publisher is merely responding to a request from client PC to download a copy of the object and embeds a unique fingerprint into the object and disseminates it to the user without a request for a license or the enforcer. "Rooted in this self-authentication, the O/S then continues to load and validate other blocks of code (including device drivers to be executed, DRM system 456 and enforcer 600, as well as, where appropriate, authenticating enforcer 600' and establishing a trust relationship with it). See column 20, lines 9-14. Thus, the downloaded object with the embedded fingerprint upon invocation generates the license request which is followed by license issuance, verification and eventually enforcement.

Second, Appellant concedes "although Venkatesan may teach the use of a publisher key, Venkatesan also fails to teach of suggest associating a product private key and public key with the software product (Brief at p. 16)." As illustrated in Figure 8 of Venkatesan, the publisher embeds a unique fingerprint into each copy of n watermarks associated with the object including a publisher (vendor) identification (a certified public key PKvid) and a product identification

key (PID) (column 13, lines 25-34, column 14, lines 31-34). As detailed in Venkatesan, "to use a protected object the license must pass through the verifier 620 which will first verify the signature in the license, then extract the rights vector, PID value and the symmetric encryption key (column 23, lines 1-22; column 24, lines 9-46 - please note that "secret key" is synonymous with private key). As is well known in the cryptographic art and disclosed in the background of the reference, "[d]epending on the specific cipher used, this secret can be, e.g., a simple key known only to a sender and a recipient, or can be a **private key** of a public/private key pair (column 3, lines 37-48; emphasis added)." The cited reference discloses that a "secret value" that may represent a public/private pair key would be associated with the software certificate (see columns 5-8; figure 5 and associated text).

Appellant further argues "Venkatesan's secret key is symmetric, i.e., there is only one rather than "a product private key and public key" as claimed (Brief at p. 17)." Indeed the key pair claimed and discussed above includes the secret key and the publisher public key.

Moreover, Appellant concedes that Venkatesan provides product identification (PID) and a certified public key but argues that the PID is indicated to be a value rather than a key. Id. As indicated on column 24, line 24, the PID is a product identification value that forms a portion of the watermark in the object, the watermark keys being (VID, PID).

Appellant further argues "Venkatesan also fails to address providing security for the license request" since it "fails to teach or suggest digitally signing the license request (Brief at p. 18)." This contention is without merit since Figure 5, clearly indicates that the license request 545 is signed 555 by the publisher before being transmitted to the client.

ii) Claims 24-26 are clearly anticipated by Venkatesan

As per claim 24, Appellant contends that the cited reference fails to disclose a "chaining of certificates (Brief at p. 19)." On the contrary, Venkatesan discloses, "[a]t run time, the key manager, in turn, checks integrity of all other critical components of enforcer 600 using digital signatures of their expected vendors. To achieve this, O/S 454 can utilize an authenticated boot process to assure its own security and then establish necessary chains of trust among various components of the O/S and particularly throughout enforcer 600 and DRM system 456 (column 19, lines 25-56)."

Appellant further contends Venkatesan fails to tie the publisher certificate to the certificate authority certificate (Brief at p. 19). Appellant indicates, "[t]he elegance of the solution is that it allows the certificate authority to control how publishers publish the software product, allows software publishers to control how end-users use their protected software products, and prevents one software publisher from authorizing a software product from another software publisher." Id. This is clearly disclosed in the cited reference, because without providing a cryptographic tie with the authority, software piracy and illegal access would be prevalent. Beginning on column 16, line 55, Venkatesan discloses by querying its user database, the publisher could learn the identity of the client PC, instruct the certificate authority to revoke a software certificate held by the PC for use with that particular key. Without a link between the publisher and the certificate authority, piracy would be possible and enforcement questionable.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Bradley Bayat
Primary Examiner
Art Unit 3621

Conferees:

Andrew Fischer, SPE 3621

Kambiz Abdi, SPE 3692